ボット対策事業運用ポリシー

２００６年１２月１日　V1.0

サイバークリーンセンター運営委員会

＜目次＞

１．　本ポリシーの位置づけ …… 1
２．　本事業の目的 …… 1
３．　本事業の参加者 …… 1
４．　業務運用 …… 3
　１）　運営委員会
　２）　検体収集者
　３）　検体等管理者
　４）　動的解析者
　５）　注意喚起者
　６）　対策情報配付者
　７）　対策情報管理者
　８）　対策情報作成者
　９）　詳細分析者
　１０）　検体最終保管者
　１１）　検体再配付事務管理者
５．　検体、及び検体情報の取扱い及び再配付のルール…… 7
６．　統計情報/評価 …… 7

１．本ポリシーの位置づけ

本「ボット対策事業運用ポリシー」は、ボット対策事業を運営するに当たり、本事業に参加する各事業主体の担当業務、及び各業務間の関連を明確にすることを目的とする。本ポリシーは事業全体に関わる基本仕様を記載するものであり、各業務における詳細な仕様に関しては、別途、検討、調整を行い、資料を作成するものとする。

また、事業期間中は、原則として、本ポリシーに則った運営を行うこととするが、やむを得ず変更せざるを得ない事由が発生した場合は、サイバークリーンセンター運営委員会の了承のもと、改訂を行うこととする。

２．本事業の目的

（１）本事業は、ボットネットを利用した不正な行為による被害の拡大を防止するため、以下の作業を遂行することを目的とする。

ア　ボットなどの Malware を検体（プログラム）として収集

イ　検体の分析、並びに駆除ツール及び対策情報(以下、「対策情報」という）の作成

ウ　感染ユーザへの告知、及び駆除の推奨

エ　ボットに関する詳細分析情報の作成、及び公開（対策情報の一般公開を含む。）

（２）この事業における対策情報の作成は、民間事業者によるサービス提供の障害となることがないよう、原則として、Malware の収集時において民間事業者が市場に提供している対策ソフト又は駆除ツールでは対策ができないものを対象とする。

３．本事業の参加者

本事業における参加者、及びそれぞれが担当する業務の概要を以下に示す。

（１）サイバークリーンセンター運営委員会（以下「運営委員会」という。）：本事業に関わる運営方針の決定、推進状況の把握、及び関連諸案件に係る対応の方針を決定する。また、検体再配付先機関になることを希望する者からの申請に対する承認を行う。

（２）検体収集者：ボット等の Malware を収集するため、Malware が感染対象とする擬餌的なインターネット環境（ハニーポット）を構築する。捕獲した Malware を検体として検体等管理者等の後工程に引き継ぐ。また、検体を捕獲した事象についても攻撃事象として後工程に引き継ぐ。

（３）検体等管理者：検体収集者から入手した検体、及び当該検体に関係する攻撃事象、並びに対策情報管理者から入手した対策情報等の総務省の所管に係る作業のために必要となる情報を一元的に管理する。また、各検体について市販の対策ソフト等による対策の可否を確認する。

（４）動的解析者：検体収集者が収集した検体を動的解析環境に移送し、実際に動作するかを確認する。動作する検体を峻別し、検体等管理者等の後工程に引き継ぐ。

（５）注意喚起管理者：検体等管理者から入手した攻撃事象情報に基づいて、本事業参加インターネットプロバイダが行う以下の作業の管理を行う。

ア　感染ユーザの特定

イ　感染ユーザに対する注意喚起メールの送信

また、注意喚起管理者は、感染ユーザにおけるMalware駆除の実行状況の進捗を管理し、事業参加インターネットプロバイダに通知する。

（６）対策情報配付者：対策情報配付者は、感染ユーザ用Webサイト及び一般公開用Webサイトを構築･運用し、検体等管理者から入手した対策情報を、感染ユーザ及び一般ユーザに対して配付する。

（７）対策情報管理者：検体等管理者から入手した検体等の情報、対策情報、及び分析結果に関する情報等の経済産業省が所管する作業のために必要となる情報を一元的に管理する。また、詳細分析情報などの分析情報をもとに対策情報を作成すべき検体を特定し、対策情報作成者に作成を指示する。作成した対策情報を検体等管理者に送付し、対策情報作成状況、及び詳細分析結果の管理を行う。

（８）対策情報作成者：対策情報管理者から入手した検体について解析を行い、対策情報管理者からの指示に従って、一般の用に供するための対策情報を作成する。

（９）詳細分析者：対策情報管理者がより詳細な分析が必要であると判断した検体について、Malwareが使用する脆弱性や振る舞い、利用されている技術などについて静的解析技術を使用して詳細な解析を行う。また、解析によって得られた情報をもとに、より効果的な対策や効率の良い分析手法の研究などを併せて行う。

（１０）検体最終保管者：本事業において収集した検体を長期間にわたり、保管する。

（１１）検体再配付事務管理者：本事業にて収集した検体を利用して、一般ユーザに対してパターンファイル又は対策情報の提供を行う組織(以下、「検体再配付先機関」という)が、本ポリシーに基づいた機能を果たすための関連する確認や処理結果に関する事務を行う。

４．業務運用

（１）運営委員会

①運営委員会の構成

「ボット対策事業」を所管する総務省、経済産業省、及び設置要領に基づき選任された委員から構成される。

②運営委員会の開催

運営委員会設置要領に基づき、定期的に開催する。

③事業推進に関する意思決定

「ボット対策事業」の遂行に関する各事業参加者からの種々の提案、報告について、決定又は承認を行う。

④検体再配付先機関の承認

検体再配付事務管理者からの提案に基づき、検体再配付先機関になることを希望する者からの申請に対する承認を行う。

⑤検体再配付先機関からのフィードバックの承認

検体再配付事務管理者から報告された検体再配付先機関のフィードバックの内容に基づき、検体再配付先機関の妥当性を判断する。

運営委員会が検体再配付の目的を十分に果たしていないと判断した検体再配付先機関については、上記④号の承認を取り消し、その旨を公表することができる。

（２）検体収集者

①検体確認作業

検体の一意な管理を行うため、収集した検体のハッシュ値を計算し、検体を捕捉した時刻のタイムスタンプを付与する。

②攻撃事象確認作業

検体を捕獲する際に攻撃元となっていたIPアドレス及びポート番号、攻撃先ハニーポットのIPアドレスとポート番号、利用した脆弱性等の攻撃手法や、攻撃された時刻等の情報を確認し、攻撃元となったユーザに対して注意喚起するための基本的な情報を収集する。

③ハニーポット構築・維持運用作業

(ア)Malwareが感染対象としている擬餌的なインターネット環境を構築する。

- ●市場普及率上位のOS環境を整える。
- ●広範囲なIPアドレスを付与し定期的にリナンバリングするなど、実際のユーザがインターネットに接続していると同じような状況を再現する。

(イ)セキュリティ対策の実施

- ●感染したMalwareがハニーポット以外の第三者に攻撃を行わないようセキュリティ対策を実施し、常時監視する。

●ハニーポット等の検体収集環境が第三者からのサイバー攻撃の対象となる恐れがあるため、常時セキュリティ監視を実施する。

（3）検体等管理者

①対策ソフトによる検査

検体収集者より受け取った検体を、都度、複数の市販のウイルス対策ソフトで検査し，その結果を記録する。

②攻撃事象の分類

検体収集者より受け取った攻撃事象に基づき、個々の攻撃事象それぞれに対し、それを行った感染ユーザを顧客とするインターネットプロバイダを特定する。

③検体、及び攻撃事象の保管

検体、及び当該検体に関係する攻撃事象等とを対応付けて保管する。

④検体の送付

検体、攻撃事象、ウイルス対策ソフトによる検査結果、及び動的解析者より受け取った解析結果などを一元化し、毎営業日に一回、対策情報管理者に送付する。

⑤対策情報の入手

一週間に一回、対策情報管理者より対策情報を入手し、当該対策情報に関係する検体と対応付けて保管する。

⑥攻撃事象、及び対策情報の送付

感染ユーザへの注意喚起のため、攻撃事象を注意管理者に、また、対策情報を対策情報配付者にそれぞれ定期的に送付する。

（4）動的解析者

①プログラム実行確認

ハニーポットで検体を捕獲する際に、感染時のファイル転送が不完全なものや、検体のプログラム・バグ等の機能不全により正常に動作しない検体を確認する。

②通信確認

プログラムが動作した検体が行う通信を IP 通信可能な擬似環境で観察し、検体がアクセスを試みたサイト等の情報を収集し管理する。

③動的解析環境の構築・運用作業

インターネットと接続されていない動的解析環境を構築し、毎日数十程度の検体を解析する。

（5）注意喚起管理者

①感染ユーザの情報をインターネットプロバイダに通知

検体等管理者から受け取った攻撃事象情報から感染ユーザの特定に必要な情報を抽出し、事業参加インターネットプロバイダに通知する。

②注意喚起メールの送信指示

事業参加インターネットプロバイダに対し、注意喚起メールの送信を指示する。注意喚起メールは、感染ユーザが一つ又はそれ以上の Malware に感染していることを通知し、感染者用 Web サイトから対策情報を入手して当該 Malware を駆除することを促す内容とする。また、注意喚起メールの送信数などを統計情報として保管する。

③進捗の管理

対策情報配付者から受け取った進捗情報に従って、個々の感染ユーザが Malware 駆除のどの段階まで実行したかについて進捗状況を管理する。

（6）対策情報配付者

①対策情報の配付

検体等管理者から受け取った対策情報を、感染ユーザ及び一般ユーザからの要求に応じて配付する。また、感染ユーザ用 Web サイト及び一般用 Web サイトへのアクセス数や対策情報の配付数などを統計情報として保管する。

②進捗情報の送付

感染ユーザ用 Web サイトにアクセスした感染ユーザが、Malware 駆除のどの段階まで実行したかを示す進捗情報を、適時、注意喚起者に送付する。

③感染ユーザ用 Web サイト及び一般用 Web サイトの構築・運用

ある Malware の感染ユーザに対して, 当該 Malware 用対策情報を提供するための感染ユーザ用 Web サイトを構築・運用する。また、広く一般ユーザに対して、既開発の対策情報を提供する一般用 Web サイトも併せて構築・運用する。

（7）対策情報管理者

①検体、及び検体情報の入手

事業参加者間において設定されたスケジュールに従い（毎営業日に一回)、検体ファイルアーカイブを検体等管理者から入手する。

②検体、及び検体情報の登録、及び対策情報作成指示

入手した検体、及び検体情報を検体等の情報を管理するシステムの対策情報作成者用外部環境に登録する。登録した検体のうち対策情報を作成する検体を検体 ID により特定して、事業参加者間において設定されたスケジュールに従い（毎営業日に一回)、対策情報作成者に作成指示を行う。

併せて、検体再配付先機関その他の検体利用機関への提供のための外部提供用環境への記録を行う。

③対策情報、及び公開用分析情報の登録、対策情報配付者への送付

(8)-④において対策情報作成者が対策情報作成者用外部提供環境に登録した対策情報、及び公

開用分析情報を事業参加者間において設定されたスケジュールに従い（一週間に一回)、検体等の情報を管理するシステムに登録するとともに、対策情報配付者宛に送付する。

④検体の検体再配付先機関への提供

(7)-②において外部提供用環境に登録された検体を検体再配付先機関へ提供する。

（８）対策情報作成者

①検体の入手

事業参加者間で設定されたスケジュールに従い（毎営業日に一回)、上記(7)-②で記録された検体、検体情報、及び対策情報作成指示情報を入手する。

②対策情報、及び公開用分析情報の作成

対策情報管理者から入手した検体について、作成指示の内容に従い、対策情報を作成する。

③対策情報の品質確保

対策情報は、一般消費者に提供されている製品に準じる信頼性や操作性等の品質を確保する。

④対策情報又は対策情報作成不能コメントの送付

作成した対策情報を事業参加者間において設定されたスケジュールに従い、対策情報作成者用外部提供環境に記録する。

作成指示に従って対策情報等を作成することができない場合は、その旨、及び理由を速やかに対策情報管理者に連絡する。

（９）詳細分析者

①詳細分析

対策情報管理者の判断により、又は他の事業参加者からの要請を踏まえ、公開用対策情報の範囲を超える詳細な分析が必要となる検体について、詳細分析を行う。

②詳細分析情報の共有

詳細分析によって得られた分析結果は、各事業参加者へ提供する。

（１０）検体最終保管者

①検体の保管

検体最終保管者は、対策情報管理者の検体等を管理するシステムへアクセスし、その外部提供用環境から検体を入手し、外部媒体に記録して保管する。

（１１）検体再配付事務管理者

①検体再配付先機関の管理

検体再配付先機関の登録管理等の事務手続き及び台帳管理等の関連する諸事務を行う。

登録管理事務手続きには以下のものを含む。

(ア)検体再配付先機関となることを希望する者からの申請を受付け、検体再配付先機関として以下

の要件を満たすかどうかを確認し、その結果を運営委員会に付すこと。

●我が国に設立された法人であって、ウイルス対策ソフトの供給（対策情報の配付を含む。）及びサービス（パターンファイルの提供等）の事業を１年以上実施している者であること。

●検体の厳格な管理基準があること

●我が国内に、技術スタッフを擁する解析部署があり、パターンファイルの作成が可能なこと

(イ)検体再配付先機関からの報告に基づき、運営委員会が、パターンファイルへの反映率が不十分であると判断した場合に、検体再配付先機関に対して、反映率の改善計画の提出を求め、提出された計画を運営委員会に報告すること。

(ウ)運営委員会が、検体再配付先機関における検体又は検体情報の管理状況に疑義があると認めた場合に、事情聴取の場を設け、運営委員会メンバーとともに事情聴取すること。

(エ)検体再配付先機関における検体又は検体情報の管理に不備があると認める場合、又はパターンファイルへの反映率改善計画が一定期間内に提出されない場合に、検体の再配付を一時的に停止するための事務を行うこと。運営委員会が承認するまでの間は、当該一時停止は、回復しないこと。

(オ)申請内容に虚偽があったことが判明した場合、第三者（本事業遂行のための分析作業等の外注先を除く。）に対して検体又は検体情報を配付した場合又は検体の再配付を一時的に停止した期間が１年を超えた場合には、運営委員会の承認を経て登録削除についての事務を行うこと

②検体再配付先機関からのフィードバックの管理

検体再配付先機関からの、検体の保管・削除の状況、複製の有無、パターンファイルへの反映状況に関するフィードバックの取りまとめの管理等の諸事務を行う。フィードバックの内容は運営委員会に報告を行う。

５．検体、及び検体情報の取扱い及び再配付のルール

（１）本事業の各参加者は、検体、及び検体情報等が本ポリシーによって権限を与えられている者以外の者に漏洩することが無いよう、十分なセキュリティレベルを確保した環境において検体、及び検体情報を取り扱わなければならない。

（２）本事業の各参加者は、運営委員会における協議により、必要性が認められた場合を除き、移送を受けた検体、及び検体情報等を本事業の参加者以外に提供しない。また、本事業の遂行のための分析作業等を本事業の参加者以外の第三者に外注する場合には、当該事業者に対し、上記(1)と同様の検体の管理義務を課すものとする。

６．統計情報/評価

（１）統計情報

各作業の担当者は協力して、事業の運用過程における以下の統計情報を定期的に運営委員会に提

出する。以下の項目は、２００６年度の報告内容とし、次年度以降は別途、検討する。

・収集検体数
・駆除可能な検体数
・注意喚起対象ユーザ数
・一般公開用 Web サイトからの対策情報の入手数

（2）評価

本事業の各参加者は、それぞれの評価基準に則って、各年度の終了時に事業評価を実施する。

以上